Report di Laboratorio: Exploit Telnet con Metasploit

Analisi Vulnerabilità e Post-Exploitation su Target Metasploitable 2

Josh Van Edward D. Abanico

21 gennaio 2026

Sommario

Il presente documento illustra le attività di Penetration Testing condotte sul servizio Telnet esposto dalla macchina target Metasploitable 2. L'attività si suddivide in scansione del servizio, ottenimento dell'accesso tramite credenziali predefinite e successiva escalation della sessione a Meterpreter, come richiesto dalle specifiche operative.

Indice

1 Obiettivo dell'Esercitazione

L'obiettivo primario è analizzare e sfruttare le debolezze del protocollo Telnet su un sistema legacy o mal configurato. Utilizzando il framework **Metasploit**, condurremo un attacco strutturato in quattro fasi:

1. Scansione e identificazione della versione del servizio.
2. Attacco di dizionario/login per ottenere accesso iniziale.
3. Interazione con la sessione shell creata.
4. Upgrade della sessione da shell semplice a Meterpreter.

2 Fase 1: Scansione del Servizio Telnet

In questa prima fase, è stato utilizzato il modulo ausiliario di Metasploit per identificare la versione del servizio Telnet in esecuzione sulla macchina target.

Modulo utilizzato: `auxiliary/scanner/telnet/telnet_version`

Di seguito viene mostrata la configurazione delle opzioni (RHOSTS) e l'output della scansione che conferma la presenza del servizio.

Figura 1: Rilevamento della versione Telnet sul target.

3 Fase 2: Autenticazione e Creazione della Sessione

Identificato il servizio, si è proceduto al tentativo di accesso utilizzando credenziali note o predefinite, sfruttando il modulo di login di Metasploit.

Modulo utilizzato: `auxiliary/scanner/telnet/telnet_login`

3.1 Configurazione dei Parametri

Sono stati impostati i seguenti parametri critici:

- **RHOSTS**: Indirizzo IP della macchina Metasploitable.

- **USERNAME/PASSWORD**: Credenziali note per il test (es. msfadmin).
- **STOP_ON_SUCCESS**: Impostato su `true` per arrestare il bruteforce al primo successo.

L'esecuzione del modulo ha prodotto l'apertura di una sessione di comando valida, come evidenziato nello screenshot seguente.

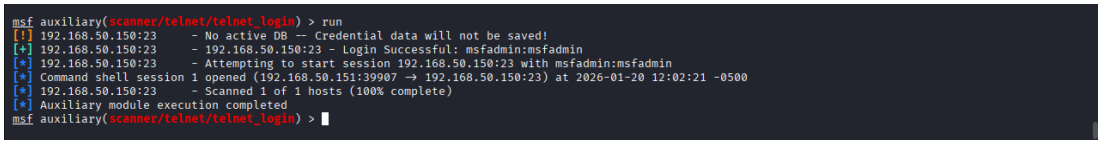

Figura 2: Login effettuato con successo e apertura della sessione.

4 Fase 3: Gestione delle Sessioni

Dopo aver ottenuto l'accesso, è stata verificata la stabilità della connessione. Utilizzando il comando `sessions -l`, è stato possibile visualizzare la lista delle sessioni attive. Successivamente, si è interagito con la sessione specifica tramite `sessions -i <ID>`.

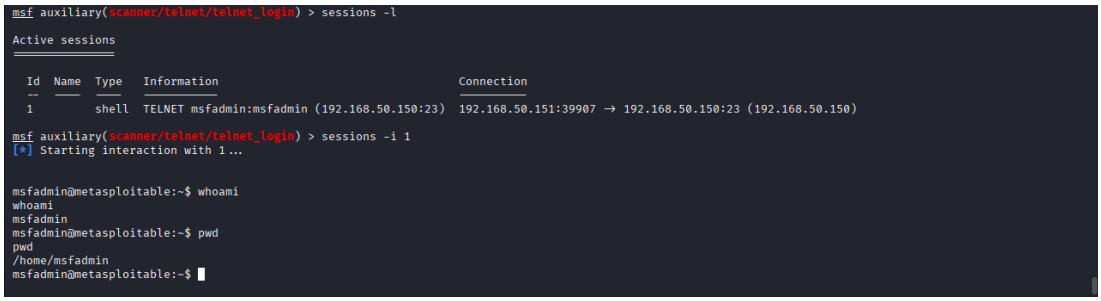

Figura 3: Elenco sessioni attive e interazione con la shell Telnet.

5 Fase 4: Upgrade della Sessione a Meterpreter

L'ultima fase ha previsto l'elevazione della qualità della connessione, trasformando la shell di base (limitata) in una sessione **Meterpreter**, che offre funzionalità avanzate di post-exploitation.

Procedura:

1. La sessione attiva è stata messa in background (`Ctrl+Z`).
2. È stato selezionato il modulo: `post/multi/manage/shell_to_meterpreter`.
3. Configurazione dell'opzione `SESSION` con l'ID della sessione Telnet precedente.

Lo screenshot sottostante mostra l'esecuzione del modulo post e la conferma dell'apertura della nuova sessione Meterpreter.

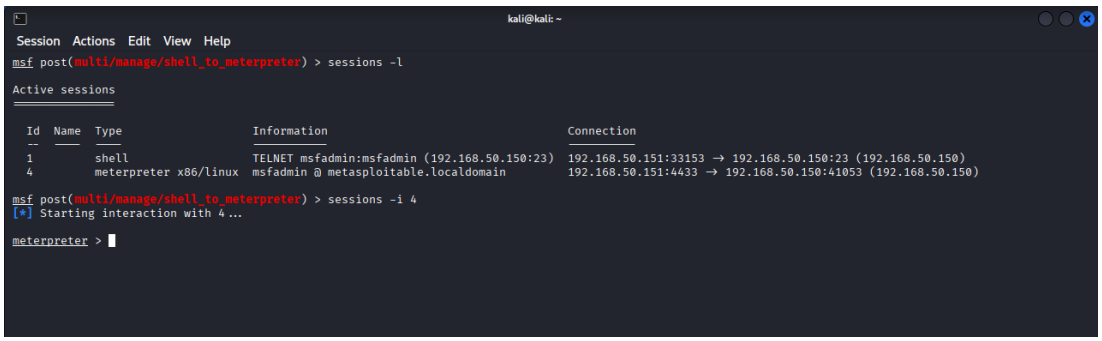

Figura 4: Upgrade riuscito: apertura della sessione Meterpreter.

6 Conclusioni

L'esercitazione ha dimostrato la vulnerabilità intrinseca del protocollo Telnet, che trasmette dati in chiaro, e la facilità con cui strumenti automatizzati come Metasploit possono sfruttare configurazioni di default. L'upgrade a Meterpreter ha confermato come un accesso iniziale a bassi privilegi o su protocolli obsoleti possa rapidamente evolvere in un controllo completo del sistema target.